Unauthorized Disclosures:

Controlled Unclassified Information unauthorized disclosures, how to prevent and report Incidents.

This is what we are going to be covering here today. First, What is Controlled Unclassified Information, why is it important to protect it, what are the possible impacts to national security, what is the difference between leaks, espionage, spills, what are the safeguarding measures necessary to protect CUI, what is the insider threat and the indicators related to possible compromise of CUI, and also what are the reporting requirements and obligations of the employee.

First, we are going to be talking about: What is Controlled Unclassified Information. CUI is a term that we use in the government to describe the type of information that we protect. Information that requires in accordance with a law, regulation, or government wide policy. The CUI Registry, which can be found at archives.gov/CUI provides detailed information on the types of CUI or information that we protect under this program. The specific laws, regulations, and government wide policies related to those information types can also be found there. First, CUI includes but is not limited to Privacy, including health information, tax information, law enforcement, critical infrastructure, export control, financial, intelligence, privilege, unclassified nuclear, procurement and acquisition. This is just the start of all the different types of CUI that can be protected.

Why do we protect CUI? First, we protect CUI because there is a law, regulation, or government wide policy that calls for its protection. Secondly, we have to recognize that if we fail to protect CUI it will have serious adverse effects on organizations, organizational operations, assets, or possibly the individuals working within those organizations. We have also seen that when there is a loss or an incident involving CUI there has been a significant financial loss to the government, the organization, and the American people. Lastly, when there is a loss or improper safeguarding of CUI it has been shown to have a direct impact on the national security of the United States.

Impacts to the National Security. A lot of you are already familiar with OPM data breach. This was a significant security or a significant CUI incident that affected over 21 million individuals and ended up costing the government over 350 million dollars to mitigate (and this is to notify and protect those impacted)

Next we are going into leaks, espionage, and data spills. First, it's important to note the difference between these so you can identify the type of incident that you are possibly reporting or coming in contact with. Leaks are where CUI is deliberately disclosed (like in the case of reporting to the media). If someone were to disclose CUI to the media that would be a leak. Espionage would be where an individual or individuals took active steps to obtain or transmit CUI from an organization. A data spill would be the willful, negligent, or inadvertent disclosure of CUI across computer systems, such as over the internet or through email. A data spill would also where CUI could possibly be posted to a social media site.

There a number of measures in place to protect CUI, these safeguarding measures are stipulated in agency policy and procedure. These safeguarding measures include everything from document marking, email encryption, physical and electronic safeguarding's, to the types of locks and safeguards that we use to protect our physical environments.

The CUI Registry, a little bit more on this, is a summary of what we protect under the CUI program. It is a catalogue of all the information types that fall under the program and that require protection in accordance with a law, regulation, or government wide policy. The CUI registry is a resource to federal agencies and to non-federal entities supporting the federal government and includes not only descriptions of these laws, regulations, and government wide polices and the categories of information but also training modules that speak to the program that speak to the various safeguarding measures that are required to ensure its protection.

Generally speaking, CUI must be safeguarded and the purpose of safeguarding is to prevent unauthorized access. Agency policy and procedure will specify the specific measures and protection requirements for agency personnel. Safeguarding measures that are authorized and accredited for classified information are also sufficient for protecting CUI.

In the Physical environment, we have to be aware of our surroundings, you have to make sure that the spaces where we handle and work with CUI are only accessed by authorized individuals. This means that our spaces must have acceptable controls in place to prevent or detect unauthorized access. Measures such as using administrative assistants to control access to a space or key control or electronic access devices are commonly used throughout agencies. Now, throughout the government and throughout non-federal entities supporting the government for the protection of CUI there should never be a situation or an instance where unauthorized individuals are given direct access to CUI. There should be some measure, individual, or mechanism in place to prevent or detect access.

In the electronic environment it is very important that we ensure that the information stored on systems and networks are also compartmentalized and protected according to an individual's lawful government purpose for access for that information. So a common practice will be or has been to develop and maintain dedicated network sites, sharepoint sites, or possibly intranet sites where unauthorized individuals are prevented from accessing such information. What I have on this slide here shows some of the common barriers that are in place to prevent unauthorized access.

Now lastly we are going to be talking about the insider. An insider of course is any individual who has access to government resource, personnel, facilities, information, equipment, networks, or systems. Now, the insider threat is somebody who happens to be on the inside and uses their position to gain unauthorized access this information. As authorized individuals we need to be aware these folks and we need to know the indicators so that way we can hopefully stop or deter them from accessing and extracting this information from the government. Some of the indicators include, but are not limited to: a general disregard for security procedures and principles, seeking access outside of the scope of an individual's current responsibilities, attempting to enter or access sensitive areas where CUI is stored, discussed, or processed, inconsistent working hours (staying too late, or arriving too early), an unusual insistence on working in private. Also, behavioral conditions such as someone who is depressed or disgruntled could serve as an indicator of someone who could possibly be engaging in activities that could place CUI in danger.

Employees are required to report any actual or suspected mishandling of CUI and also any suspicious behaviors among the workforce that could potentially compromise or lead to the compromise of CUI. It is important that you know who to report these incidents to, often times within organizations it is your security officer or security manager.

When in doubt, report it!

Now, in summary, everyone should review any applicable agency and organizational policies, familiarize yourself with what you currently are protecting and how to protect that information in accordance with agency policies, and be on the lookout for any suspicious behaviors among the workforce, and most importantly know how to this information to the proper officials within your organization. Thank you very much for your time.